USAID
FROM THE AMERICAN PEOPLE

EURASIAN DIGITAL FOUNDATION

EURASIA FOUNDATION

СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ НАЦИОНАЛЬНОГО И ЗАРУБЕЖНОГО ЗАКОНОДАТЕЛЬСТВА ПО ОПЕРАТИВНОМУ РЕАГИРОВАНИЮ ПРИ УТЕЧКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Данное исследование/отчет/публикация стало возможным благодаря помощи американского народа, оказанной через Агентство США по международному развитию (USAID). Eurasian Digital Foundation несет ответственность за содержание публикации, которое не обязательно отражает позицию USAID или Правительства США.

ВВЕДЕНИЕ **3**

Институт персональных данных в Казахстане и международные принципы его защиты **3**

АНАЛИЗ НАЦИОНАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ **8**

2020-2021 годы: актуализация законодательства в сфере защиты персональных данных **8**

2022 год: процедура уведомления об утечке персональных данных **12**

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ КАЗАХСТАНСКОГО ЗАКОНОДАТЕЛЬСТВА О ПЕРСОНАЛЬНЫХ ДАННЫХ **14**

Административная ответственность **14**

Уголовная ответственность **16**

ОТВЕТСТВЕННОСТИ В СТРАНАХ ЕВРОПЕЙСКОГО СОЮЗА **20**

ЗАКОНОТВОРЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГРУЗИИ **23**

ЗАКЛЮЧЕНИЕ И РЕКОМЕНДАЦИИ **26**

ВВЕДЕНИЕ

Задача по формированию законодательства, комплексно обеспечивающее правовое регулирование проблем, связанных с информацией персонального характера, относится к числу наиболее сложных задач государства.

В настоящее время в Казахстане законодательно не урегулированы вопросы оперативного реагирования при утечке персональных данных, необходимые для минимизации последствий такой утечки, а также не установлены обязательства по уведомлению уполномоченного органа для собственника и (или) оператора. Кроме этого, в национальном понятийном аппарате отсутствует определение термина "утечка".

Главным образом было исследовано национальное и зарубежное законодательство, в том числе законодательная инициатива Грузии, а также лучшие практики в сфере защиты персональных данных при их утечке. На данное время остается актуальным вопрос по механизму привлечения к ответственности оператора, а также по определению пределов ответственности оператора персональных данных в Республике Казахстан при утечке персональных данных.

Настоящий документ подготовлен в рамках проекта "Институт развития защиты персональных данных" экспертами Русланом Дайырбековым и Елжаном Кабышевым при поддержке Фонда Евразия в рамках программы "Социальные инновации в Центральной Азии", финансируемой Агентством США по международному развитию (USAID).

ИНСТИТУТ ПЕРСОНАЛЬНЫХ ДАННЫХ В КАЗАХСТАНЕ И МЕЖДУНАРОДНЫЕ ПРИНЦИПЫ ЕГО ЗАЩИТЫ

Распространенные нарушения прав физических лиц в отношении их персональных данных, неоднократные случаи массовой утечки сведений из информационных систем органов государственной власти и негосударственных организаций очевидным образом требовали адекватного ответа от отечественного законодателя.

Расширение возможностей информационно-коммуникационных технологий позволило создать принципиально новые формы сбора и хранения персональных данных, а также обмена ими. Были разработаны международные базовые принципы защиты данных, включая обязательства по

- справедливому и законному получению персональной информации;
- ограничению сферы ее использования первоначально определенной целью; обеспечению того, чтобы ее обработка имела надлежащий, соответствующий и не чрезмерный характер;
- обеспечению ее точности;
- обеспечению безопасности;

- ее уничтожению в случае отсутствия потребностей в ней;
- представлению частным лицам права доступа к информации о них и права ходатайствовать о внесении в нее исправлений.

Комитет по правам человека в своем замечании общего порядка № 16 четко указал, что вышеуказанные принципы относятся к праву на неприкосновенность частной жизни, но защита данных также начинает выделяться в качестве отдельного права человека.

С учетом назначения и содержания этих принципов, по отношению к рассматриваемой теме утечек персональных данных, их можно объединить в несколько групп:

- определения прав субъектов данных;
- установления обязательств государства по обеспечению правовой охраны персональных данных.

В первую группу принципов, согласно предложенной их классификации, входят принципы, определяющие права субъектов персональных данных. Во-первых, исходя из критериев законности обработки персональных данных, это принцип согласия субъекта данных на сбор и обработку информации о нем. Во-вторых, на основании политики и практики открытости в отношении работы с персональными данными, это принципы закрепляющие права субъектов данных быть осведомленным о существовании базы данных о нем; о главных целях такой базы; об органе (должностном лице, юридическом лице) обеспечивающем обработку данных; об источнике получения данных; о категории используемых данных; о получателях его данных в случае их передачи. И, в третьих, принципы, основанные на обеспечении права личного участия субъекта данных в работе с его персональными данными. Это принципы, устанавливающие гарантии прав субъекта данных на доступ к своим данным.

Следующая группа принципов касается обеспечения защиты персональных данных. Конвенция Совета Европы "О защите частных лиц в отношении автоматизированной обработки данных личного характера" №108 от 28 января 1981 года закрепляет несколько норм, устанавливающих обязанности государств ратифицировавших Конвенцию принимать необходимые меры для того, чтобы основные принципы защиты данных, предусмотренные Конвенцией, были реализованы в национальном праве. Директива Европейского Парламента и Совета Европы 95/46/ЕС "О защите личности в отношениях обработки персональных данных и свободном обращении этих данных" развивает положения Конвенции, устанавливая принцип конфиденциальности обработки персональных данных.

Международным правом закреплено право индивида прибегать к помощи, в случае незаконного использования данных, а также право запрещать использование данных при определенных обстоятельствах.

К сожалению, следует констатировать факт, что принцип, устанавливающий гарантии прав субъекта персональных данных на обеспечение права личного участия с его персональными данными, нуждается в дальнейшей глубокой проработке отечественными законодателями.

Суммируя вышесказанное в нижеследующей таблице можно сравнить какие международные стандарты защиты персональных данных в случае их утечек реализованы в Законе "О песональных данных и их защите"("О ПДиЗ"), а какие – нет.

Сравнение стандарта защиты права человека, закрепленного в международном праве, со стандартом этой защиты, определенным в Законе "О ПДиЗ".

Международные принципы работы с персональными данными	Положения Закона "О персональных данных и их защите"
Принцип согласия субъекта данных на сбор и обработку информации о нем	Данный принцип содержится в статье 7, согласно которой сбор, обработка персональных данных осуществляются собственником и (или) оператором с согласия субъекта или его законного представителя, кроме случаев, предусмотренных статьей 9 Закона "О ПДиЗ". Согласно ст. 9 Закона, обработка осуществляется без согласия следующих случаях: • осуществление деятельности государственными органами (пункты 1, 2, 3, 9, 9-1, 9-2); • реализации международных договоров (п. 4); • защиты конституционных прав и свобод (п. 5); • осуществление деятельности СМИ (п. 6); • составления реестра бизнес-партнеров (п. 9-3) • в случае требований иных законов (п. 7, 8 и 10).
Принцип согласия субъекта данных на сбор и обработку информации о нем	Статья 24 Закона определяет право субъекта персональных данных знать о наличии у собственника и (или) оператора, а также третьего лица своих персональных данных, а также получать информацию, содержащую: 1. подтверждение факта, цели, источников, способов сбора и обработки персональных данных; 2. перечень персональных данных; 3. сроки обработки персональных данных, в том числе сроки их хранения. Статья 25 Закона устанавливает обязанность собственника и (или) оператора сообщать информацию, относящуюся к субъекту, в установленные законом сроки со дня получения обращения субъекта или его законного представителя.

Принцип достоверности персональных данных (право на исправление неверных данных, или уничтожение их в случае их незаконной, необоснованной или неточной регистрации)	Принцип достоверности установлен в статье 13: *"Изменение и дополнение персональных данных осуществляются собственником и (или) оператором на основании обращения (запроса) субъекта или его законного представителя либо в иных случаях, предусмотренных законами Республики Казахстан".* Статья 25 Закона определяет обязанность собственника и (или) оператора в течение одного рабочего дня: *"изменить и (или) дополнить персональные данные на основании соответствующих документов, подтверждающих их достоверность, или уничтожить персональные данные при невозможности их изменения и (или) дополнения".* Пп. 2) п.1 ст. 24 гласит, что *"Субъект имеет право требовать от собственника и (или) оператора изменения и дополнения своих персональных данных при наличии оснований, подтвержденных соответствующими документами".*
Принцип срока хранения данных	Статья 12 Закона гласит, что хранение персональных данных осуществляется собственником и (или) оператором, а также третьим лицом в базе, которая хранится на территории Республики Казахстан. Срок хранения персональных данных определяется датой достижения целей их сбора и обработки, если иное не предусмотрено законодательством Республики Казахстан.
Принцип, устанавливающий гарантии прав субъекта данных на доступ к своим данным	Согласно статье 10 доступ к персональным данным определяется условиями согласия субъекта или его законного представителя, предоставленного собственнику и (или) оператору на их сбор и обработку, если иное не предусмотрено законодательством Республики Казахстан. Доступ к персональным данным должен быть запрещен, если собственник и (или) оператор, и (или) третье лицо отказываются принять на себя обязательства по обеспечению выполнения требований Закона или не могут их обеспечить. Согласно статье 21, защита персональных данных осуществляется путем применения комплекса мер, в том числе правовых, организационных и технических, в целях (среди прочих) реализации права на доступ к ним. Также, статья 25 Закона определяет обязанность собственника и (или) оператора сообщать информацию, относящуюся к субъекту, в предусмотренные законом сроки со дня получения обращения субъекта или его законного представителя.

Принцип, основанный на обеспечении права личного участия субъекта данных в работе с его персональными данными	Пункт 8 статьи 25 Закона определяет обязанность собственника и (или) операторов в течение одного рабочего дня: • изменить и (или) дополнить персональные данные на основании соответствующих документов, подтверждающих их достоверность, или уничтожить персональные данные при невозможности их изменения и (или) дополнения; • блокировать персональные данные, относящиеся к субъекту, в случае наличия информации о нарушении условий их сбора, обработки; • уничтожить персональные данные в случае подтверждения факта их сбора, обработки с нарушением законодательства Республики Казахстан, а также в иных случаях, установленных настоящим Законом и иными нормативными правовыми актами Республики Казахстан; • снять блокирование персональных данных в случае неподтверждения факта нарушения условий сбора, обработки персональных данных.
Принцип гласности операций по обработке данных	Отсутствует в Законе
Принцип конфиденциальности обработки персональных данных	Статья 11 Закона гласит, что *"Собственники и (или) операторы, а также третьи лица, получающие доступ к персональным данным ограниченного доступа, обеспечивают их конфиденциальность путем соблюдения требований не допускать их распространения без согласия субъекта или его законного представителя либо наличия иного законного основания".*

АНАЛИЗ НАЦИОНАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 18 Конституции Республики Казахстан закрепляет в себе право человека на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства. Также указано, что человек имеет право на тайну личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Однако ограничения этого права допускаются только в случаях и в порядке, прямо установленных законом.

С 2013 года в Казахстане действует специальный Закон "О персональных данных и их защите", который регулирует общественные отношения, возникающие в связи со сбором, обработкой, хранением персональных данных.

Ниже мы анализируем как с 2020 года изменялось законодательство о персональных данных.

2020-2021 ГОДЫ: АКТУАЛИЗАЦИЯ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Законодательство Республики Казахстан с 2020 по 2021 годы было дополнено новыми нормативными правовыми актами и положениями в сфере защиты персональных данных.

7 июля 2020 года вступил в силу Кодекс "О здоровье народа и системе здравоохранения", где впервые использовано понятие "персональные медицинские данные" - это персональные данные, содержащие сведения о здоровье физического лица и оказанных ему медицинских услугах, зафиксированные на электронных, бумажных или иных материальных носителях.

С принятием Закона Республики Казахстан "О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий" от 25 июня 2020 года № 347-VI ЗРК был образован новый уполномоченный государственный орган в сфере защиты персональных данных - Управление по защите персональных данных, входящий в Комитет информационной безопасности при Министерстве цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан (МЦРИАП РК). Управление, как следует из названия, занимается вопросами защиты прав субъектов персональных данных.

Создание уполномоченного органа в сфере персональных данных является революционным для развития отечественного правового института персональных данных.

В его функции входит разработка порядка осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных; рассмотрение обращений субъекта или его законного представителя о соответствии содержания персональных данных и способов их обработки целям их обработки; принятие мер по привлечению лиц, допустивших нарушения законодательства Республики Казахстан о персональных данных и их защите к ответственности; требования от собственника и (или) оператора, а также третьего лица уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных; осуществление мер, направленных на совершенствование защиты прав субъектов и утверждение правил сбора, обработки персональных данных.

30 декабря 2021 года президентом Республики Казахстан был подписан Закон Республики Казахстан "О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам торговой деятельности, развития биржевой торговли и защиты персональных данных" № 96-VII ЗРК, который внес следующие процедуры и нормы:

- государственный и негосударственный сервисы контроля доступа к персональным данным;
- расширение функционала "Сервиса контроля доступа к персональным данным" регистрацией действий должностных лиц.

Об уведомлении субъектов персональных данных упоминается следующих случаях:

1. Государственным сервисом обеспечиваются:
    a. уведомление субъекта о действиях с его персональными данными, содержащимися в объектах информатизации государственных органов и (или) государственных юридических лиц (доступ, просмотр, изменение, дополнение, передача, блокирование, уничтожение);
    b. уведомление субъекта об инициаторах запросов на доступ (сбор и обработку) к его персональным данным, содержащимся в объектах информатизации государственных органов и (или) государственных юридических лиц, через государственный сервис (в случаях, предусмотренных подпунктами 4), 6), 8) и 9-3) статьи 9 закона).
2. Негосударственным сервисом обеспечиваются:
    a. уведомление субъекта о действиях с его персональными данными;
    b. уведомление субъекта о доступе третьих лиц к его персональным данным;
3. При наличии условия об уведомлении субъекта о передаче его персональных данных третьему лицу контроле в течение десяти рабочих дней уведомляют об этом субъекта, если иное не предусмотрено законами Республики Казахстан.

Однако ни в одной статье закона не указано об уведомлении субъектов при незаконной обработке их персональных данных, вместе с тем, не установлены пределы ответственности оператора в случае невыполнения им обязанности по уведомлению субъектов персональных данных об их утечке.

Проанализировав зарубежные нормы, устанавливающие пределы ответственности оператора за нарушение безопасности персональных данных и обязанность уведомления надзорного органа и субъекта персональных сведений, авторы настоящей работы отмечают, необходимость ужесточения мер ответственности за нарушение безопасности персональных данных путем повышения пределов ответственности, а именно увеличением размера административных штрафов. Тем самым обозначив масштабность проблем, возникающих при утечке персональных данных граждан.

В связи с тем, что на сегодняшний день у уполномоченного органа по защите персональных данных отсутствует возможность инициировать проверку на предмет законности сбора и обработки персональных данных, депутатом Смышляевой Е.В. была инициирована поправка, наделяющая МЦРИАП РК полномочием по осуществлению государственного контроля за соблюдением законодательства Республики Казахстан о персональных данных и их защите в соответствии с Предпринимательским кодексом РК.

Комитет информационной безопасности (КИБ) МЦРИАП вправе принимать меры исключительно при обращениях и жалобах и по уже совершившимся правонарушениям: когда персональные данные незаконно попали третьим лицам, распространены неопределенному кругу лиц и т.д.

Вместе с тем, ранее органы прокуратуры привлекали правонарушителей к ответственности в соответствии со статьей 79 КоАП РК при нарушении законодательства РК о персональных данных и их защите, а также до настоящего времени осуществляют надзор в этой сфере.

При этом для органов прокуратуры не требуется наличие в Предпринимательском кодексе Республики Казахстан функции государственного контроля для проведения внеплановых проверок, в свою очередь, такая функция государственного контроля необходима для уполномоченного органа (КИБ МЦРИАП).

Данная мера необходима для недопущения незаконного сбора персональных данных граждан, их использования в незаявленных и коммерческих целях, а также пресечения нарушений, предусмотренных законодательством об информатизации, о персональных данных и их защите.

Благодаря законопроекту, по словам министра цифрового развития, инноваций и аэрокосмической промышленности РК Багдата Мусина:

“Появится возможность для проведения комплексного анализа курируемых отраслей, актуализации данных в государственных базах, принятия обоснованных и эффективных управленческих решений в режиме онлайн. Одновременно, для обеспечения защиты персональных данных будут ужесточаться требования к применению информационно-коммуникационных технологий. Для этого законопроектом предлагается признать информационные системы, осуществляющие сбор, обработку и хранение персональных данных, критически важными объектами информационно-коммуникационной инфраструктуры и повысить требования к их защищенности”.

Автор данного дополнения, Смышляева Е.В, обосновала необходимость поправки тем фактом, что до определения уполномоченного органа в сфере защиты персональных данных органами прокуратуры по статье 79 КоАП РК с 2016 по 2018 годы рассмотрено 0 административных дел и в 2019 году рассмотрено 3 административных дела. Наряду с этим, с момента определения (июнь 2020 года) МЦРИАП уполномоченным органом в сфере защиты персональных данных по настоящее время рассмотрено более 210 жалоб субъектов персональных данных, то есть граждан (публикация персональных данных общедоступными интернет-ресурсами, такими как adata.kz, fa-fa.kz, kompra.kz; незаконное распространение персональных данных в различных группах мессенджеров и социальных сетях; использование персональных данных без согласия их субъектов и несовместимых их целям сбора и т.д.), 157 из которых удовлетворены.

Однако, в связи с наличием противоречий в законодательстве и отсутствием функции государственного контроля в сфере защиты персональных данных более 50 жалоб остались без удовлетворения. Вышеуказанные меры ответственности могут применяться должным образом, при наличии независимого специализированного органа в сфере защиты персональных данных субъектов, в рамках полномочий которого осуществляется контроль действий контролера персональных сведений и расследование при обнаружении нарушения закона о персональных данных.

Также авторы работы отмечают, что наделение полномочиями госконтроля за соблюдением законодательства о персональных данных и их защите позволит гражданам быть осведомленными об утечке своих данных. В целях развития защиты персональных данных, необходимо повысить информированность граждан об утечке персональных данных также путем внесения изменений в соответствующие нормы РК, в которых устанавливается обязанность оператора уведомлять казахстанцев в случае утечки персональных данных, включая пределы ответственности за несоблюдение этих норм.

Согласно статье 27-1 Закона “О ПДиЗ”, уполномоченный орган в пределах своей компетенции принимает меры по привлечению лиц, допустивших нарушения законодательства РК о персональных данных и их защите, к ответственности, установленной законами РК. При этом, в соответствии со статьей 28 вышеуказанного законодательства органы прокуратуры осуществляют высший надзор за соблюдением законности в сфере защиты персональных данных.

Безусловно, следует приветствовать наличие ряда положительных правовых норм, направленных на обеспечение конфиденциальности персональных данных граждан в вышеуказан-

ных поправках. Так, отдельного внимания заслуживает норма закрепляющая расширенное, по сравнению с ранее действующей редакцией, толкование "Принципа определенности целей сбора и обработки данных", закрепленного в статье 14 Закона "О ПДиЗ". Дополнения в статью 7 данного закона гласят, что *"обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Таким образом, впервые в национальном законодательстве был закреплен международный принцип "минимизации данных".*

До недавнего времени, обеспечение многих организационных и технических мер, направленных на минимизацию рисков причинения вреда гражданам в случае утечки их персональных данных, были оставлены на усмотрение самих операторов.

18 января 2020 года Правительство Республики Казахстан своим постановлением № 12 "Изменения и дополнения, которые вносятся в некоторые решения Правительства Республики Казахстан", утвердило новую редакцию "Правил осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных", которые, среди прочего, закрепили обязанность соблюдать собственником и (или) оператором законодательства Республики Казахстан о персональных данных, путем назначения лица, ответственного за организацию обработки персональных данных.

Кроме этого, Постановлением Правительства Республики Казахстан от 30 апреля 2021 года № 285, вышеуказанные правила по обеспечению мер по защите персональных данных, были дополнены обязанностью собственника и оператора предоставлять доступ государственной технической службе к объектам информатизации, использующим, хранящим, обрабатывающим и распространяющим персональные данные ограниченного доступа, для осуществления "обследования обеспечения защищенности процессов хранения, обработки и распространения персональных данных ограниченного доступа".

2022 ГОД: ПРОЦЕДУРА УВЕДОМЛЕНИЯ ОБ УТЕЧКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Эксперты проекта приняли участие в нескольких рабочих встречах в качестве приглашенных экспертов в области приватности.

22 и 28 апреля 2022 года под председательством депутата мажилиса парламента Смышляевой Е. В. прошли заседания рабочей группы по проекту закона "О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам стимулирования инноваций, развития цифровизации и информационной безопасности".

В связи с тем, что законодательно не урегулированы вопросы оперативного реагирования при утечке персональных данных, необходимые для минимизации последствий такой утечки, а также понимая важность проведения комплексной работы в этих случаях, авторы проекта закона предложили установить для собственника и (или) оператора обязательства по уведомлению уполномоченного органа.

В рамках обсуждения проекта закона Управлением по защите персональных данных КИБ МЦРИАП было инициировано дополнение в статью 25 ЗРК "О ПДиЗ", в следующей редакции:

"11) в течение двух рабочих дней уведомить уполномоченный орган об утечке персональных данных с указанием контактных данных лица, ответственного за организацию обработки персональных данных".

В свою очередь, эксперты проекта, концептуально поддержав вышеуказанную новеллу, обратили внимание законодателей на статью 33 General Data Protection Regulation (GDPR, Общий регламент по защите данных) "Уведомление надзорного органа о нарушении безопасности персональных данных" в части необходимости закрепления требования собственника и оператора по обработке персональных данных — "задокументировать любые нарушения безопасности персональных данных, в том числе их обстоятельства, последствия и меры, принятые для исправления ситуации".

В связи с тем, что в национальном понятийном аппарате отсутствует определение "утечки", депутаты вернули данную норму на доработку. На последующем заседании рабочей группы, после согласования с соответствующими государственными органами, депутатам на обсуждение представили доработанную редакцию дополнения в статью 25, в которой слово "утечка" было заменено на "нарушения защиты персональных данных", в следующей редакции:

"11) в течение двух рабочих дней уведомить уполномоченный орган о выявленных нарушениях защиты персональных данных с указанием контактных данных лица, ответственного за организацию обработки персональных данных".

Однако эксперты обратили внимание на пункт 11) статьи 1 Закона "О ПДиЗ" от 21 мая 2013 года, который определяет *"защиту персональных данных как комплекс мер, в том числе правовых, организационных и технических, осуществляемых в целях, установленных настоящим Законом"*. Таким образом, согласно смыслу предлагаемой редакции, любое нарушение вышеуказанных мер предполагает уведомление уполномоченного органа, что является обременительной и избыточной мерой.

В этой связи, эксперты поддержали определение "утечки", предложенное Управлением по защите персональных данных КИБ МЦРИАП, а именно:
"утечка персональных данных – нарушение безопасности персональных данных, влекущих к случайному или незаконному распространению, изменению, дополнению, использованию, обезличиванию, блокированию и уничтожению или доступу к персональным данным".

В конечном итоге, соответствующие изменения по процедуре уведомления регулятора об утечке персональных данных не вошли в закон, который был принят 14 июля 2022 года.

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ КАЗАХСТАНСКОГО ЗАКОНОДАТЕЛЬСТВА О ПЕРСОНАЛЬНЫХ ДАННЫХ

В Республике Казахстан предусмотрена административная и уголовная ответственности за нарушение законодательства о персональных данных и их защите.

АДМИНИСТРАТИВНАЯ ОТВЕТСТВЕННОСТЬ

Статья 79 "Нарушение законодательства Республики Казахстан о персональных данных и их защите" Кодекса об административных правонарушений Республики Казахстан (далее - КоАП РК) предусматривает ответственность, к которым должны привлекаться лица, нарушившие Закон Республики Казахстан "О персональных данных и их защите" от 21 мая 2013 года N 94-V (далее - ЗРК "О ПДиЗ"). В настоящей статье указаны пределы ответственности нарушителя, об этом подробнее в нижеуказанной таблице.

Часть 1 ст. 79 КоАП РК
Незаконные сбор и (или) обработка персональных данных, если эти деяния не содержат признаков уголовно наказуемого деяния:

Субъект-нарушитель	Размер штрафа (в МРП на 2022 год)	Размер штрафа (в тенге на 2022 год)
Физические лица (ФЛ)	10	30 630
Должностные лица, частные нотариусы, частные судебных исполнители (ЧСИ), адвокаты, субъекты малого предпринимательства, некоммерческие организации (НКО)	20	61 260
Субъекты среднего предпринимательства	30	91 890
Субъекты крупного предпринимательства	70	214 410

Часть 2 настоящей статьи КоАП РК Те же деяния, совершенные собственником, оператором или третьим лицом с использованием своего служебного положения, если эти действия не влекут установленную законом уголовную ответственность:		
ФЛ	50	153 150
Должностные лица, субъекты малого предпринимательства, НКО	75	229 725
Субъекты среднего предпринимательства	100	306 300
Субъекты крупного предпринимательства	200	612 600
Часть 3 настоящей статьи КоАП РК Несоблюдение собственником, оператором или третьим лицом мер по защите персональных данных, если это деяние не содержит признаков уголовно наказуемого деяния:		
ФЛ	50	153 150
Должностные лица, субъекты малого предпринимательства, НКО	100	306 300
Субъекты среднего предпринимательства	150	459 450
Субъекты крупного предпринимательства	200	612 600
Часть 4 настоящей статьи КоАП РК Деяние, предусмотренное частью третьей настоящей статьи, повлекшее утерю, незаконный сбор и (или) обработку персональных данных, если эти деяния не влекут установленную законом уголовную ответственность:		
ФЛ	200	612 600
Должностные лица, субъекты малого предпринимательства, НКО	500	1 531 500
Субъекты среднего предпринимательства	700	2 144 100
Субъекты крупного предпринимательства	1 000	3 063 000

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ

Ответственность за противоправные действия, которые нарушают ЗРК "О ПДиЗ", предусмотрены не только в КоАП РК, но также и в Уголовном кодексе Республики Казахстан (далее - УК РК), в частности:

- Глава 3 "Уголовные правонарушения против конституционных и иных прав и свобод человека и гражданина" ст. 147 "Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите";
- Глава 7 "Уголовные правонарушения в сфере информатизации и связи" ст. 211 "Неправомерное распространение электронных информационных ресурсов ограниченного доступа".

В нижеуказанной таблице предусмотрены наказания за совершение уголовных преступлений.

ст. 147 УК РК
Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите

Часть статьи	Наказание					
	Штраф (в МРП и в тенге)	Исправительные работы	Общественные работы	Ограничение свободы	Лишение свободы	Атимия[1]
Часть 1 Несоблюдение мер по защите персональных данных лицом, на которое возложена обязанность принятия таких мер, если это деяние причинило существенный вред правам и законным интересам лиц	3 000 МРП / 9 189 000 тенге	3 000 МРП / 9 189 000 тенге	600 часов	2 года	2 года	до 3 лет

[1] Атимия (гр. atimia) - в Древней Греции полное или частичное лишение гражданских прав. Атимия происходила либо вследствие наказания, наложенного судом за определенные проступки и преступления, либо непосредственно вытекала из неисполнения определенных обязанностей по отношению к государству, Большой юридический словарь, дата: 27 сентября 2022 года, источник: https://jurisprudence.academic.ru/7743/%D0%90%D1%82%D0%B8%D0%BC%D0%B8%D1%8F
В данном документе термин "атимия" применяется для сокращения определения дополнительного наказания за уголовное преступление: "лишение права занимать определенную должность или заниматься определенной деятельностью" (пп. 3 п. 3 ст. 40 УК РК)

Часть 2 Незаконное собирание сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо причинение существенного вреда правам и законным интересам лица в результате незаконных сбора и (или) обработки (за исключением распространения) иных персональных данных	5 000 МРП / 15 315 000 тенге	5 000 МРП / 15 315 000 тенге	800 часов	3 года	3 года	x
Часть 3 Деяния, предусмотренные частью 2 настоящей статьи, совершенные лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, либо путем незаконного доступа к электронным информационным ресурсам, информационной системе или незаконного перехвата информации, передаваемой по сети телекоммуникаций, либо в целях извлечения выгод и преимуществ для себя или для других лиц, или организаций, а равно в отношении лица или его близких в связи с осуществлением данным лицом служебной деятельности либо выполнением профессионального или общественного долга с целью воспрепятствования такой деятельности или из мести за нее	x	x	x	x	5 лет	x
Часть 4 Распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо причинение существенного вреда правам и законным интересам лица в результате незаконного распространения иных персональных данных	x	x	x	x	от 3 до 6 лет	x

Часть 5 Совершение действий, предусмотренных частью 4 настоящей статьи, в публичном выступлении, публично демонстрирующемся произведении, в средствах массовой информации или с использованием сетей телекоммуникаций, в том числе через Интернет, а равно в отношении лица или его близких в связи с осуществлением данным лицом служебной деятельности либо выполнением профессионального или общественного долга с целью воспрепятствования такой деятельности или из мести за нее	x	x	x	x	от 3 до 7 лет	x

ст. 211 УК РК
Неправомерное распространение электронных информационных ресурсов ограниченного доступа

Часть статьи	Наказание						
	Штраф (в МРП и в тенге)	Исправительные работы	Общественные работы	Арест	Ограничение свободы	Лишение свободы	Атимия
Часть 1 Неправомерное распространение электронных информационных ресурсов, содержащих персональные данные граждан или иные сведения, доступ к которым ограничен законами Республики Казахстан или их собственником или владельцем	200 МРП / 612 600 тенге	200 МРП / 612 600 тенге	180 часов	50 суток с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового	x	x	до 3 лет

Часть 2 То же деяние, совершенное: 1) группой лиц по предварительному сговору; 2) из корыстных побуждений; 3) лицом с использованием своего служебного положения	x	x	1 200 часов	x	5 лет	5 лет	до 3 лет
Часть 3 Деяния, предусмотренные частями первой или второй настоящей статьи: 1) совершенные преступной группой; 2) повлекшие тяжкие последствия	x	x	x	x	x	от 3 до 7 лет	до 5 лет

ОТВЕТСТВЕННОСТИ В СТРАНАХ ЕВРОПЕЙСКОГО СОЮЗА

Правовая система, прогрессирующих стран по защите персональных данных основывается на Общем регламенте защиты персональных данных Европейского Союза (GDPR), поскольку данный регламент разработан в целях внесения фундаментальных изменений способов обработки персональных данных по всей Европе.

GDPR устанавливает ответственность за нарушение законодательства.

Согласно пункту 4 статьи 83 GDPR, за несоблюдение мер для обеспечения уровня безопасности защиты персональных данных и за неуведомление субъекта налагается административный штраф в размере до 10 000 000 евро, в случае субъекта хозяйствования — до 2% от общего годового мирового оборота за предыдущий финансовый год, в зависимости от того, что выше. В странах Европейского Союза пределом административной ответственности за вышеизложенные деяния составляет 20 000 000 евро или 4% от общего годового мирового оборота, что указывает на высокую значимость обеспечения безопасности персональных данных. Такой подход способствует эффективному предотвращению нарушений норм, обеспечивающих безопасность персональных данных.

Что касается уголовной ответственности в зарубежных странах, пределы ответственности устанавливаются согласно национальному законодательству. К примеру, согласно разделу 41 Закона Франции от 6 января 1978 г. № 78-17 "О защите данных" к уголовной ответственности на срок от шести месяцев до пяти лет может быть привлечено лицо, не выполнившее правила соблюдения мер по обеспечению защиты персональных данных, нарушающих частной жизни физических лиц. К ответственности за такие преступления привлекаются и те лица, которые неосмотрительно или небрежно разгласили или разрешили разглашать персональные данные.

В странах Европейского Союза в соответствии с подпунктом i) пункта 2 статьи 58 GDPR, административные штрафы за утечку персональных данных уполномочен налагать надзорный орган. Роль такого надзорного органа установлена в статье 51 GDPR. Надзорные органы являются независимыми государственными органами, которые контролируют, посредством следственных и корректирующих полномочий, применение закона о защите данных. Они предоставляют экспертные консультации по вопросам защиты данных и рассматривают жалобы, поданные на нарушения GDPR и соответствующих национальных законов. В каждом государстве-члене ЕС есть по одному такому надзорному органу, который несет ответственность за мониторинг применения GDPR в целях обеспечения защиты фундаментальных прав и свобод физических лиц в отношении обработки, а также свободного движения персональных данных на территории ЕС. Например: Комиссия по защите персональных данных в Болгарии, Хорватское агентство по защите персональных данных, Управление омбудсмена по защите данных во Франции, Испанская организация по защите данных , и т.д.

Брауде-Золотарев М. Ю в своем труде "Персональные данные в государственных информационных ресурсах" отмечает, что реформирование правового режима уполномоченного органа в сфере контроля за обработкой персональных данных допустимо введением нового органа государственной власти, занимающегося деятельностью исключительно по линии "контроль – надзор – защита персональных данных".

Одним из важнейших обязанностей оператора по обработке персональных данных является уведомление органа, уполномоченного следить за соблюдением безопасности и сохранности персональных данных субъектов. Уведомление такого органа до совершения действий с персональными данными предусмотрено и Директивой Европейского сообщества № 95/46/ЕС, в частности в статье 18, где говорится о том, что оператор или его представитель должен уведомить надзорный орган перед осуществлением любой полностью или частично автоматизированной операции по обработке операций, предназначенных, чтобы служить одной цели или нескольким связанным целям.

Невыполнение указанной обязанности может караться серьезным штрафом или даже рассматриваться как уголовное преступление (например, в Великобритании, Италии, Нидерландах, Франции).

Согласно GDPR, уведомление надзорного органа о любой утечке персональных данных должно быть осуществлено без неоправданной задержки и, по возможности, в течение 72 часов после того, как об этом стало известно, за исключением случаев, когда инцидент "маловероятно приведет к риску для прав и свобод физических лиц". В уведомлении должна быть указана определенная информация о нарушении, включая категории и приблизительное количество соответствующих субъектов данных, а также вероятные последствия нарушения (статья 33 GDPR). Аналогичным образом, за некоторыми исключениями, должны быть уведомлены отдельные субъекты персональных данных, данное уведомление должно содержать ту же информацию, которую необходимо сообщить в надзорный орган (статья 34).

На практике зарубежных стран наблюдается иной подход по привлечению к ответственности контролера персональных данных, способствующий благотворному обеспечению защиты прав персональных данных. В странах Европейского Союза в соответствии с GDPR каждое государство-член должно иметь один или несколько независимых государственных органов, осуществляющие надзорные полномочия и ответственные за контроль применения Регламента. В частности, такие надзорные органы являются независимыми. В деле С-518/07, КОМИССИЯ V. ГЕРМАНИЯ, 9 марта 2010 г., Европейский суд разъяснил, что независимость означает статус, который гарантирует, что заинтересованный орган может действовать совершенно свободно,без каких-либо инструкций или давления. Требование независимости касается не только отношений между надзорными органами и органами, подлежащими этому надзору. Прилагательное "полный" подразумевает полномочия по принятию решений, независимые и свободные от любого прямого или косвенного внешнего влияния на надзорный орган, в том числе со стороны государства.

К примеру, в Ирландии таким надзорным органом является Комиссия по защите данных. Данная Комиссия отслеживает и обеспечивает соблюдение GDPR; способствует информированию общественности о правилах и правах, связанных с обработкой данных; консультирует правительство по вопросам защиты данных; повышает осведомленность контролеров и обработчиков об их обязанностях; рассматривает жалобы и проводит расследования, связанные с соблюдением закона о защите данных.

Также, Комиссия имеет право приказать любому контролеру или обработчику предоставить информацию, которая требуется властям для оценки соблюдения Регламента. Он может проводить расследования в отношении контролеров и обработчиков в форме аудита данных, включая доступ к помещениям контролера или обработчика.

Согласно преамбуле 117 GDPR, надзорный орган должен быть наделен правом исполнять свои полномочия на основе полной самостоятельности. Ярким примером является наложение штрафа, Нидерландским надзорным органом по защите данных в размере 565 000 евро на Министерство иностранных дел Нидерландов. В рамках своего расследования Нидерландский надзорный орган по защите данных обнаружил, что Национальная визовая информационная система страдает серьезными недостатками безопасности, а Министерство иностранных дел Нидерландов в среднем обрабатывало 530 000 заявлений на получение визы в год. Нидерландский надзорный орган по защите данных заявил, что персональные данные, которые обрабатываются в ходе рассмотрения заявления недостаточно защищены. В ходе расследования данный орган выявил, что Министерство иностранных дел Нидерландов знало о недостатках безопасности в визовой системе, однако, не приняло мер по корректировке безопасности. Таким образом, вышеуказанная практика свидетельствует о независимости, самостоятельности надзорного органа, так как он, проводя на самостоятельной основе расследования, привлек к ответственности одного из высших органов государственной власти за нарушения безопасности персональных данных.

В 2020 году Управление по защите данных Гамбурга в соответствии со статьей 5 и 6 GDPR оштрафовало сотрудника полиции на сумму 400 евро за то, что последний сфотографировал официальную презентацию, содержащую личные данные, и поделился им в групповом чате WhatsApp. Также известен случай, произошедший 4 апреля 2022 года, когда Греческий орган по защите данных оштрафовал мэра на сумму 5000 евро на основании статьи 5 (a) GDPR. Данное высшее должностное лицо направило документы работника муниципалитета третьим лицам без его согласия.

ЗАКОНОТВОРЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГРУЗИИ

В Грузии в рамках новой законотворческой инициативы планируется определить понятие "инцидент" в Закон Грузии "О защите персональных данных" №5669-რს от 28.12.2011 года. Определение инцидента раскрывается следующим образом: *"фактическое нарушение безопасности данных или потенциальная угроза такого нарушения, которое осуществляется с использованием информационных технологий и вызывает или может привести к неправомерному или несанкционированному разглашению, повреждению, уничтожению, утрате, изменению, несанкционированному доступу, сбору/извлечение данных и которые наносят ущерб или ставят под угрозу права и/или интересы субъекта данных".*

В связи с закреплением понятия "утечка" планируется изменение статей 29 и 30 грузинского закона о защите персональных данных.

Статья 29 "Обязанность сообщить о происшествии (утечке данных) в Государственную инспекторскую службу":

1. Контроллер/обработчик данных обязан зафиксировать инцидент, его результаты и меры, принятые для решения инцидента, и не позднее 72 часов после обнаружения инцидента сообщить об этом в письменной или электронной форме Службе Государственного инспектора в порядке, определенном Государственным инспектором, за исключением случаев, когда маловероятно, что происшествие причинит вред лицу или нарушение его прав и свобод.
2. Уведомление, предусмотренное частью первой настоящей статьи, должно содержать следующие сведения:
   a. об обстоятельствах, виде и времени происшествия;
   b. в результате инцидента предполагаемые категории и объем незаконно раскрытых, поврежденных, удаленных, уничтоженных, полученных, утерянных или измененных данных, а также предполагаемые категории и количество субъектов данных, которые оказались в опасности в результате инцидента;
   c. предполагаемый ущерб, причиненный инцидентом, меры, предпринятые или запланированные контролером или обработчиком данных для его уменьшения или устранения;
   d. планирует ли контролер или обработчик данных уведомить субъекта/субъектов данных об инциденте в порядке, установленном статьей 30 настоящего Закона, и в какие сроки;
   e. контактные данные уполномоченного по защите персональных данных или иного контактного лица.

3. В случае невозможности предоставления информации, указанной в пункте 2 настоящей статьи, полностью и сразу, контролер или обработчик данных имеет право предоставлять информацию поэтапно в течение разумного периода времени по согласованию с Государственной инспекцией.
4. Если, согласно уведомлению, контролер не предоставляет или не может предоставить информацию субъекту(ам) данных, принимая во внимание обстоятельства происшествия, предполагаемый ущерб и/или количество субъектов данных, Государственный инспектор уполномочен обнародовать информацию об инциденте независимо от того, несет ли контролер данных обязанность, предусмотренную статьей 30 настоящего Закона.

Статья 30 "Обязанность информирования субъекта данных о происшествии":

1. Если инцидент может причинить существенный вред субъекту данных или поставить под угрозу его/ее основные права человека, контролер данных обязан проинформировать субъекта данных об инциденте в разумный срок после обнаружения инцидента, но не позднее 1 месяца, и предоставить ему на понятном и простом языке следующую информацию:
    a. общее описание происшествия и связанных с ним обстоятельств;
    b. возможный/неизбежный ущерб, вызванный инцидентом, принятые или планируемые меры по уменьшению или устранению ущерба;
    c. контактные данные уполномоченного по защите персональных данных или иного лица.
2. При наличии надлежащего письменного обоснования срок, предусмотренный частью первой настоящей статьи, может быть продлен не более чем на 1 месяц по согласованию с государственным инспектором.
3. Если информирование субъекта данных требует несоразмерно больших затрат или усилий, контролер данных обязан распространить информацию, указанную в части первой настоящей статьи, публично или в иной форме, которая в достаточной мере обеспечивает возможность получения информации субъектами данных.
4. Бремя доказывания выполнения обязательства по информированию субъекта данных о происшествии, предусмотренном настоящей статьей, лежит на контроллере данных.

Основные отличия между грузинскими и казахстанскими законодательными инициативами по утечкам персональным данных:

Грузия	Казахстан
Уведомление регулятора в течение 72 часов	Уведомление регулятора в течение двух рабочих дней
Уведомление регулятору должно содержать: • обстоятельства, вид и время происшествия; • категории и объем персональных данных, количество субъектов персональных данных; • предполагаемый ущерб, предпринятые меры; • план по уведомлению субъектов; • контактные данные.	Уведомление должно содержать: • факт утечки персональных данных; • контактные данные лица, ответственного за организацию обработки персональных данных.
Уведомление субъектов персональных данных	Отсутствовало в проекте закона

В Казахстане в 2022 году была инициатива о внесении понятия "утечка", сроков уведомления регулятора в рамках проекта закона "О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам стимулирования инноваций, развития цифровизации и информационной безопасности". Подробнее об этом можно ознакомиться в разделе "2022 год: процедура уведомления об утечке персональных данных".

ЗАКЛЮЧЕНИЕ И РЕКОМЕНДАЦИИ

Последние два года активно актуализируется законодательство, усиливаются права субъектов персональных данных, в том числе через призму усиления регулятора - Управление по защите персональных данных КИБ МЦРИАП РК.

На наш взгляд, учитывая все вышеуказанное, законодательство требуется в дальнейшем совершенствовании, а именно:

Рекомендация	Обоснование
Наделение полномочиями госконтроля за соблюдением законодательства о персональных данных и их защите.	У уполномоченного органа по защите персональных данных отсутствует возможность инициировать проверку на предмет законности сбора и обработки персональных данных.
Определить и предусмотреть в Законе "О ПДиЗ" понятие "утечка персональных данных".	Предусмотренное законодательством понятие "утечка персональных данных" необходимо в целях: • правильного применения норм КоАП и УК в случае допущения утечки персональных данных со стороны оператора и (или) собственника; • реализации права субъекта персональных данных на возмещение материального или морального вреда в случае утечки персональных данных.
Предусмотреть в законе порядок и процедуру уведомления регулятора в случае утечки персональных данных.	Необходимо в целях: • минимизации вреда субъектов персональных данных; • принятия оперативных мер по защите субъектов персональных данных со стороны регулятора.
Предусмотреть обязанность собственников и (или) операторов об уведомлении регулятора в случае утечки персональных данных.	Предусмотренное статьей 25 Закона "О ПДиЗ" обязательство оператора и (или) собственника по уведомлению регулятора в случае утечки персональных данных. Нарушение обязательства должно содержать предусмотренную законодательством ответственность.
Предусмотреть в законе порядок и процедуру уведомления субъектов персональных данных, чьи данные были незаконно распространены предусмотреть обязанность собственников и (или) операторов об уведомлении субъектов персональных данных, чьи данные были незаконно распространены.	Предусмотренное статьей 25 Закона "О ПДиЗ" обязательство оператора и (или) собственника по уведомлению субъектов персональных данных. Нарушение обязательства должно содержать предусмотренную законодательством ответственность.